

EQUALITY OF DEDEKIND SUMS MOD $8\mathbb{Z}$

EMMANUEL TSUKERMAN

ABSTRACT. Using a generalization due to Lerch [M. Lerch, Sur un théorème de Zolotarev. Bull. Intern. de l'Acad. François Joseph 3 (1896), 34-37] of a classical lemma of Zolotarev, employed in Zolotarev's proof of the law of quadratic reciprocity, we determine necessary and sufficient conditions for the difference of two Dedekind sums to be in $8\mathbb{Z}$. These yield new necessary conditions for equality of two Dedekind sums. In addition, we resolve a conjecture of Girstmair [Girstmair, Congruences mod 4 for the alternating sum of the partial quotients, arXiv: 1501.00655].

Keywords: Dedekind sums, Zolotarev's Lemma, Barkan-Hickerson-Knuth formula.

MSC: 11F20.

1. BACKGROUND

Dedekind sums are classical objects of study introduced by Richard Dedekind in the 19th century in his study of the η -function [Ded53]. Among many other areas of mathematics, Dedekind sums appear in: geometry (lattice point enumeration in polytopes [BR07]), topology (signature defects of manifolds [HZ74]) and algorithmic complexity (pseudo random number generators [Knu97]). To define the Dedekind sums, let

$$((x)) = \begin{cases} x - [x] - 1/2, & \text{if } x \in \mathbb{R} \setminus \mathbb{Z}; \\ 0, & \text{if } x \in \mathbb{Z}. \end{cases}$$

Then the Dedekind sum $s(a, b)$ for $a, b \in \mathbb{N}$ coprime is defined by

$$s(a, b) = \sum_{k=1}^b ((\frac{ak}{b})) ((\frac{k}{b})).$$

Recently, in [JRW11], Jabuka et al. raise the question of when two Dedekind sums $s(a_1, b)$ and $s(a_2, b)$ are equal. In the same paper, they prove the necessary condition $b \mid (a_1 a_2 - 1)(a_1 - a_2)$ for equality of two dedekind sums $s(a_1, b)$ and $s(a_2, b)$. Girstmair [Gir14] shows that this condition is equivalent to $12s(a_1, b) - 12s(a_2, b) \in \mathbb{Z}$. In [Tsu14], necessary and sufficient conditions for $12s(a_1, b) - 12s(a_2, b) \in 2\mathbb{Z}, 4\mathbb{Z}$ are given.

In this note we give necessary and sufficient conditions for $12s(a_1, b) - 12s(a_2, b) \in 8\mathbb{Z}$ by using a generalization of Zolotarev's classical lemma relating the Jacobi symbol to the sign of a special permutation¹ due to Lerch [Ler96]. Along the way, we resolve a conjecture of Girstmair about the alternating sum of partial quotients modulo 4 [Gir15].

2. PRELIMINARIES

Let $\pi_{(a,b)} \in \text{Aut}(\mathbb{Z}/b\mathbb{Z}), \pi_{(a,b)} : x \mapsto ax$. Let $[x]_b = x - b[\frac{x}{b}]$ be the function taking $x \in \mathbb{Z}/b\mathbb{Z}$ to its smallest nonnegative representative. We view $\pi_{(a,b)}$ as a permutation of $\{0, 1, \dots, b-1\}$ given by

$$\pi_{(a,b)} = \begin{pmatrix} 0 & 1 & \cdots & b-1 \\ [\pi(0)] & [\pi(1)] & \cdots & [\pi(b-1)] \end{pmatrix} = \begin{pmatrix} 0 & 1 & \cdots & b-1 \\ 0 & [a]_b & \cdots & [(b-1)a]_b \end{pmatrix}.$$

The precedent for doing so is already present in the work of Zolotarev, in which he relates the sign of $\pi_{(a,b)}$ to the Jacobi symbol and obtains a proof of the law of quadratic reciprocity (see, e.g., [RG72, pg. 38]). Let $I(a, b)$ denote the number of inversions of $\pi_{(a,b)}$.

Date: January 22, 2015.

¹The motivation behind Zolotarev's work was to produce a proof of the law of quadratic reciprocity.

Theorem 2.1. (*Zolotarev*) For odd b and $(a, b) = 1$,

$$(-1)^{I(a,b)} = \left(\frac{a}{b}\right).$$

The following result shows that the inversions of $\pi_{(a,b)}$ and Dedekind sums are closely related.

Theorem 2.2. (*Meyer*, [Mey57]) The number of inversions $I(a, b)$ of $\pi_{(a,b)}$ is equal to

$$I(a, b) = -3bs(a, b) + \frac{1}{4}(b-1)(b-2),$$

where $s(a, b)$ is the Dedekind sum.

From the reciprocity law of dedekind sums, one obtains a reciprocity law for inversions.

Theorem 2.3. (*Salié*, [Mey57, p. 163]) For all coprime $a, b \in \mathbb{N}$

$$(1) \quad 4aI(a, b) + 4bI(b, a) = (a-1)(b-1)(a+b-1).$$

Let a and b be positive integers, $a < b$. Consider the regular continued fraction expansion

$$\frac{a}{b} = [0, a_1, \dots, a_n],$$

where all digits a_1, \dots, a_n are positive integers. We assume that n is odd². We will be interested in

$$T(a, b) = \sum_{j=1}^n (-1)^{j-1} a_j$$

and

$$D(a, b) = \sum_{j=1}^n a_j.$$

With this notation,

Theorem 2.4. (*Barkan-Hickerson-Knuth formula*) Let $a, b \in \mathbb{N}$ be coprime and let $a^*a \equiv 1 \pmod{b}$ with $0 < a^* < b$. Then

$$12s(a, b) = T(a, b) + \frac{a + a^*}{b} - 3.$$

In [Ler96], Lerch improves upon Zolotarev's Lemma by determining the parity of $I(a, b)$ when b is even:

Theorem 2.5. (*Lerch*)

$$I(a, b) \equiv \begin{cases} \frac{1 - (\frac{a}{b})}{2}, & \text{if } b \text{ is odd} \\ \frac{(a-1)(b+a-1)}{4}, & \text{if } b \text{ is even} \end{cases} \pmod{2}.$$

Proof. We assume that b is even, as the result for b odd follows from Theorem 2.1. Reducing the equality

$$4aI(a, b) + 4bI(b, a) = (a-1)(b-1)(a+b-1)$$

from Theorem 2.3 modulo 8 and using the assumption that b is even yields

$$4aI(a, b) \equiv (a-1)(b-1)(a+b-1) \pmod{8}.$$

Since $a-1$ and $a+b-1$ are even,

$$aI(a, b) \equiv (b-1) \frac{(a-1)(b+a-1)}{4} \pmod{2},$$

from which the claim follows. \square

For further generalizations of Zolotarev's Lemma, see [BC14].

²If n is even, we can consider instead $[0, a_1, \dots, a_n - 1, 1]$.

3. MAIN RESULTS

As a consequence of Theorem 2.5, we are able to show the following necessary and sufficient conditions for equality of Dedekind sums mod $8\mathbb{Z}$.

Theorem 3.1. *Let $a_1, a_2 \in \mathbb{N}$ be relatively prime to $b \in \mathbb{N}$. The following are equivalent:*

- (a) $I(a_1, b) \equiv I(a_2, b) \pmod{2b}$
- (b) $3s(a_1, b) - 3s(a_2, b) \in 2\mathbb{Z}$
- (c) Let $\left(\frac{a}{b}\right)$ denote the Jacobi Symbol and define

$$\mu(a, b) = \begin{cases} \frac{1 - \left(\frac{a}{b}\right)}{2}, & \text{if } b \text{ is odd} \\ \frac{(a-1)(b+a-1)}{4}, & \text{if } b \text{ is even} \end{cases}$$

Then

$$(a_1 - a_2)(b - 1)(b + a_1a_2 - 1) \equiv 4b(a_2\mu(b, a_1) - a_1\mu(b, a_2)) \pmod{8b}.$$

We also determine $T(a, b) \pmod{8}$:

Theorem 3.2. *Let $a, b \in \mathbb{N}$ be coprime. Then*

$$bT(a, b) \equiv -4\mu(a, b) + b^2 + 2 - a - a^* \pmod{8}.$$

Reducing further to mod 4 and mod 2 resolves a conjecture of Girstmair [Gir15].

4. PROOFS AND EXAMPLES

Theorem 3.1. Let $a_1, a_2 \in \mathbb{N}$ be relatively prime to $b \in \mathbb{N}$. The following are equivalent:

- (a) $I(a_1, b) \equiv I(a_2, b) \pmod{2b}$
- (b) $3s(a_1, b) - 3s(a_2, b) \in 2\mathbb{Z}$
- (c) Let $\left(\frac{a}{b}\right)$ denote the Jacobi Symbol and define

$$\mu(a, b) = \begin{cases} \frac{1 - \left(\frac{a}{b}\right)}{2}, & \text{if } b \text{ is odd} \\ \frac{(a-1)(b+a-1)}{4}, & \text{if } b \text{ is even} \end{cases}$$

Then

$$(2) \quad (a_1 - a_2)(b - 1)(b + a_1a_2 - 1) \equiv 4b(a_2\mu(b, a_1) - a_1\mu(b, a_2)) \pmod{8b}.$$

Proof. The equivalence of 3.1(a) and 3.1(b) follows from Theorem 2.2. Reducing equation (1) of Theorem 2.3 modulo $8b$ and using Theorem 2.5 yields

$$4aI(a, b) + 4b\mu(b, a) \equiv (a - 1)(b - 1)(a + b - 1) \pmod{8b}.$$

□

That Theorem 3.1 is not a sufficient condition for the equality of two Dedekind sums is demonstrated in the following example.

Example 4.1. Take $a_1 = 1, a_2 = 15$ and $b = 49$. Then

$$\left(\frac{b}{a_1}\right) = 1, \quad \left(\frac{b}{a_2}\right) = 1.$$

We have

$$(a_1 - a_2)(b - 1)(b + a_1a_2 - 1) = -42336 = 108 \cdot 8 \cdot 49 \equiv 0 \pmod{8b}.$$

Thus we expect $3s(a_1, b) - 3s(a_2, b) \in 2\mathbb{Z}$. Indeed,

$$s(a_1, b) = \frac{188}{49}, \quad s(a_2, b) = -\frac{8}{49},$$

so that

$$3s(a_1, b) - 3s(a_2, b) = 12.$$

Equality does not hold.

Theorem 3.2. Let $a, b \in \mathbb{N}$ be coprime. Then

$$(3) \quad bT(a, b) \equiv -4\mu(a, b) + b^2 + 2 - a - a^* \pmod{8}.$$

Proof. By Theorems 2.2 and 2.4, we have

$$\begin{aligned} bT(a, b) &= 12bs(a, b) - a - a^* + 3b \\ &= -4I(a, b) + b^2 + 2 - a - a^*. \end{aligned}$$

Reducing modulo 8 and using Theorem 2.5,

$$bT(a, b) \equiv -4\mu(a, b) + b^2 + 2 - a - a^* \pmod{8}.$$

□

Let $k \in \mathbb{Z}$ satisfy $aa^* = 1 + kb$. In [Gir15], Girstmair conjectures that if $a \equiv a^* \equiv 0 \pmod{2}$, then

- (i) If a or a^* is $\equiv 2 \pmod{4}$, then $T(a, b) \equiv (b - k)/2 \pmod{4}$
- (ii) If a and a^* are both $\equiv 0 \pmod{4}$, then $T(a, b) \equiv (k - b)/2 \pmod{4}$
- (iii) If a and a^* are both $\equiv 0 \pmod{4}$, then $D(a, b)$ is odd.

We now show how this follows from Theorem 3.2. Reducing congruence (3) mod 4 gives

$$bT(a, b) \equiv b^2 + 2 - a - a^* \pmod{4}.$$

Assume first that $a \equiv a^* \equiv 0 \pmod{4}$. Then

$$bT(a, b) \equiv b^2 + 2 \equiv -1 \pmod{4} \implies T(a, b) \equiv -b^{-1} \equiv -b \pmod{4}.$$

On the other hand,

$$1 + kb \equiv 0 \pmod{8} \implies k \equiv -b \pmod{8}.$$

This proves (ii). As Girstmair notes, part (iii) follows from (ii).

Next we show (i). It suffices to prove the result when $a \equiv 2 \pmod{4}$, since $T(a, b) = T(a^*, b)$. We have

$$bT(a, b) \equiv 1 - a^* \pmod{4} \implies T(a, b) \equiv b^{-1}(1 - a^*) \equiv b(1 - a^*) \pmod{4}.$$

On the other hand,

$$\frac{b - k}{2} \equiv \frac{b - b^{-1}(aa^* - 1)}{2} \equiv b - \frac{baa^*}{2} \equiv b - ba\left(\frac{a^*}{2}\right) \equiv b - ba^* \pmod{4}.$$

This completes the proof.

This, together with the results in [Gir15], determines $T(a, b)$ and $D(a, b)$ in all cases.

Acknowledgments. The author would like to thank Kurt Girstmair and Pete Clark for helpful comments and bibliographic references.

This material is based upon work supported by the National Science Foundation Graduate Research Fellowship under Grant No. DGE 1106400. Any opinion, findings, and conclusions or recommendations expressed in this material are those of the authors(s) and do not necessarily reflect the views of the National Science Foundation.

REFERENCES

- [BC14] Adrian Brunyate and Pete L. Clark. Extending the Zolotarev–Frobenius approach to quadratic reciprocity. *The Ramanujan Journal*, pages 1–26, 2014.
- [BR07] Matthias Beck and Sinai Robins. *Computing the continuous discretely*. Undergraduate Texts in Mathematics. Springer, New York, 2007. Integer-point enumeration in polyhedra.
- [Ded53] R. Dedekind. Erläuterungen zu den fragmenten xxviii. pages 466–478, 1953. Collected Works of Bernhard Riemann.
- [Gir14] K. Girstmair. A criterion for the equality of dedekind sums mod \mathbb{Z} . *Int. J. Number Theory*, 10(3):565–568, 2014.
- [Gir15] K. Girstmair. Congruences mod 4 for the alternating sum of the partial quotients. 2015.
- [HZ74] F. Hirzebruch and D. Zagier. *The Atiyah-Singer theorem and elementary number theory*. Publish or Perish, Inc., Boston, Mass., 1974. Mathematics Lecture Series, No. 3.
- [JRW11] S. Jabuka, S. Robins, and X. Wang. When are two Dedekind sums equal? *Int. J. Number Theory*, 7(8):2197–2202, 2011.
- [Knu97] Donald E. Knuth. *The Art of Computer Programming, Volume 2 (3rd Ed.): Seminumerical Algorithms*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 1997.
- [Ler96] M. Lerch. Sur un théorème de zolotarev. *Bull. Intern. de l’Acad.*, pages 34–37, 1896.

- [Mey57] C. Meyer. ber einige anwendungen dedekindscher summen. *Journal für die reine und angewandte Mathematik*, 198:143–203, 1957.
- [RG72] H. Rademacher and E. Grosswald. *Dedekind sums*. The Mathematical Association of America, Washington, D.C., 1972. The Carus Mathematical Monographs, No. 16.
- [Tsu14] E. Tsukerman. Equality of dedekind sums mod \mathbb{Z} , $2\mathbb{Z}$ and $4\mathbb{Z}$. *International Journal of Number Theory*, 2014.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, BERKELEY, CA 94720-3840
E-mail address: `e.tsukerman@berkeley.edu`